

MEMORANDUM FOR: Deputy Director for Operations
(Attention: Eloise Page)

Deputy Director for Science and Technology
(Attention: Ernest J. Zellmer)

Director, National Foreign Assessment Center
(Attention: [REDACTED])

General Counsel

(Attention: [REDACTED])

FROM : Michael J. Malanick
Associate Deputy Director for Administration

SUBJECT : Planning for Implementation of E.O. 12065

REFERENCE : Action Plan Approved 26 July 1978 for
Implementation of E.O. 12065

Attached for your planning and guidance is a paper prepared by the Task Force concerned with implementing the provisions of E.O. 12065 concerning classification, declassification, and mandatory review. Because of the amount of work to be accomplished by 1 December 1978, it is hoped that the paper will prove useful to you in accomplishing the tasks outlined.

Michael J. Malanick

Attachment: a/s

cc: D/Sec (Attention: [REDACTED])
DTR (Attention: Harry Fitzwater)

Distribution:

Original - ADDA w/att
1 - ADDA Chrono wo/att

1 - AI/DDA w/att

1 - Each Addressee

CIA Task Force, E.O. 12065
Classification, Declassification, Mandatory Review Guidance

1. Introduction

a. The recently issued Executive Order 12065 requires that CIA as an agency with original classification authority promulgate Classification Guides (Sec. 5-403) and Declassification Guidelines (Sec. 3-402), and that they develop procedures for mandatory review of information for declassification (Sec. 3-501). The Order also requires that unclassified regulations establishing agency information security policy and unclassified guidelines for systematic declassification review shall be published in the Federal Register (Sec. 5-402). The Order further stipulates that Agency implementing regulations contain criteria explaining in narrative form the reason information needs to be protected beyond six years (Sec. 1-502).

b. The NSC draft implementing directive for the Executive Order requires that Classification Guides contain categories and subcategories of information to be protected, the level of classification to apply to each, the duration of such specified classification, and the reason for any extension of classification beyond six years.

c. The CIA Task Force concerned with implementing the classification, declassification, and mandatory review requirements noted above is currently drafting two basic papers and identifying tasks for the consideration of the three Directorates and NFAC.

2. Classification Guides

Conceptually the Task Force envisages three different levels of classification guides.

a. Agency Classification Guide

This Guide will set forth broad categories of intelligence information based upon the seven classification requirements a-g (Sec. 1-301). These categories will be generally common to all Directorates. The guide will be unclassified and require Deputy Director and DCI approval. It appears likely that it will have to be published in the Federal Register. Whether classification designations and duration of classification have to be assigned to each category of information in the basic Agency guide remains to be resolved. If such assignment is required, a variable classification designation from Confidential to Top Secret for each category would seem appropriate combined with a duration of up to 20 years.

b. Directorate Classification Guides

These guides will establish subcategories of intelligence information based upon the Agency Classification Guide and will contain information generally common to all components of a Directorate. They may be classified or unclassified and will be approved by the individual Deputy Directors. Each subcategory of information will require a determination as to the level of classification, the duration of the classification, and the reason for any extension of classification beyond six years.

c. Office (or equivalent) Classification Guides

These will further expand upon the subcategories of information contained in the Directorate Classification Guides and will reflect the needs and concerns of individual components of each Directorate. They may be classified or unclassified and will be approved by the Office Directors or Chiefs of the individual components and ultimately by the pertinent Deputy Director. Each such subcategory of information will require a determination as to the level of classification, the duration of the classification, and the reason for any extension of classification beyond six years.

3. Draft of Agency Classification Guide and Task Force Comments for Directorate Consideration

a. A draft Agency Classification Guide will be distributed to Directorates o/a 1 September 1978 and Directorate comments are requested by 18 September 1978. This tight deadline is necessary because the Agency Classification Guide will serve as a starting point for Directorate and Office guides.

b. It should be noted that E.O. 12065 recognizes that there may be national security categories of information other than those set forth in a-f of the E.O. which require protection against unauthorized disclosure. Directorates should carefully examine categories a-f to determine if additional (g) categories are needed to meet their requirements. Any such additional categories require DCI approval.

c. As noted in paragraph 4 below, the Task Force is attempting to dovetail its draft Agency Classification Guide with Directorate guidelines for systematic declassification prepared in late 1977. It is therefore recommended that Directorates review their guides for declassification in conjunction with their review of the Task Force draft Agency Classification Guide.

d. In the preparation of Directorate and Office Classification Guides, information requiring protection must be categorized to the extent possible. The Classification Guides should state which of the classification designations (i.e., Top Secret, Secret, or Confidential) apply to each category of information. A statement covering the duration of classification when such duration is to exceed six years and the reason for such extension is also required.

e. Although Directorate and Office Classification Guides may be classified to the level necessary, lower classifications are encouraged considering the intended wide use of the guides.

f. Directorates are reminded that the significance in developing comprehensive Classification Guides lies in the authority extended by the E.O. to permit derivative classification to individuals not provided original classification authority (Sec. 2 of the Order). Every original classification must include both a decision that the information concerns one or more of the criteria a-g described in Sec. 1-301 of the Order, and a decision that disclosure of the information reasonably could be expected to cause one of the three levels (grave, serious, identifiable) of damage described in Sec. 1-1 of the Order. The decision involved in each step must be considered separate and distinct from that of the other.

4. Guidelines for Systematic Declassification Review

Each Directorate in late 1977 approved a guideline for systematic review for declassification.

a. The Task Force is drawing from the four Directorate guidelines and preparing an unclassified Agency Declassification Guideline for publication in the Federal Register. The draft Agency guideline will be sent to Directorates for comment later in the year inasmuch as we have until 1 May 1979 to accomplish this objective.

b. The guides for classification and declassification should dovetail. The Task Force is therefore drawing from the Directorate guidelines for declassification in its preparation of the basic guide for classification. It follows that Directorates may desire to review their guidelines for declassification when they review the basic classification guide prepared by the Task Force.

c. Directorate guidelines for declassification previously prepared as unclassified contain in some cases information that should be classified. Also if categories of information needing protection are not covered in the guides for declassification, documents containing such information are automatically declassified after 20 years or 30 years for foreign government information. It is recommended therefore that Directorates review their guidelines for declassification for both comprehensiveness and classification of content. Directorates may prepare classified supplementary guidelines for declassification as required.

d. The Task Force will prepare a draft special systematic review guideline for foreign government information.

e. Special procedures for systematic review and declassification of classified cryptologic information will be developed by the Secretary of Defense. The DCI is responsible for developing special procedures for systematic review and declassification of classified information concerning the identities of clandestine human agents. The Task Force will be looking to the DDO for input in developing the latter guideline which will be binding on the Intelligence Community.

5. Mandatory Review Procedures

It is anticipated that the current modus operandi between the Information and Privacy Staff and Agency components for handling mandatory review requests along with FOIA and Privacy Act requests will be continued. The Task Force will be responsible for drafting a paper describing these procedures for mandatory review to conform with Sec. 3-5 of the Order.

6. Task Force Assistance

Questions on this paper should be referred to Directorate Focal Point Officers who are available to provide assistance as may be required.

26 July 78

ACTION PLAN FOR
DDA ASSIGNED TASKS
ASSOCIATED WITH THE IMPLEMENTATION OF
EXECUTIVE ORDER 12065

The DDA assigned tasks associated with the implementation of the new Executive Order have been grouped under one of the following four general headings:

- Classification/Declassification/Mandatory Review
- Markings
- Training
- Safeguarding

TASK FORCES

Individual task forces will be established to handle each of the four areas listed above. The first three task forces will be chaired by ISAS representatives while the fourth will be chaired by a representative from the Office of Security. C/ISAS will function as the coordinator between all task forces.

A representative from each of the four Directorates and OGC will be appointed to each task force to form the basic working group. Additional members can be requested by each Chairman if and when the need arises. Once formed, each task force will be organized internally to handle their individual program elements in the most efficient manner.

DIRECTORATE SUPPORT

To obtain and maintain the shortest possible response time from the four Directorates, it is recommended that the job responsibilities for the four individuals who are currently functioning as the senior Declassification Focal Point Officers for each Directorate be expanded to include all coordination activities associated with the development and implementation of this program. It is further recommended that where practical, those individuals within each Directorate that were tasked with helping to develop declassification guidelines, be designated to assist the Declassification Focal Point Officers with all coordination activities. The above structure worked extremely well in developing the declassification guidelines and should function equally as well in helping to develop and coordinate this program.

ACTUAL PROGRAM IMPLEMENTATION

Within the DDA, records management personnel will be playing an extremely important role in the actual implementation of the new E.O. This role will be to act as the means for transmitting to Agency personnel the actual instructions on what actions are required and how they are to

be done. In this role they will also serve as convenient points of contact for the multitude of questions that are sure to be raised as actual implementation efforts move forward. Involvement of these personnel will be through the Directorate Records Management Officer who will participate in and be kept fully informed on all aspects of the implementation program.

How this program will be implemented within the other Directorates is something that should be decided upon at the earliest possible date.

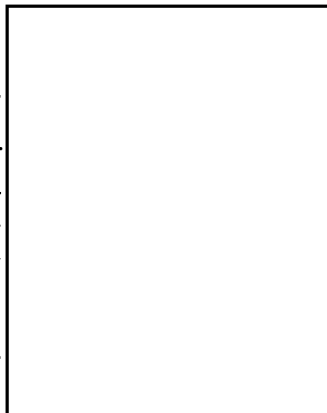
WORK ASSIGNMENTS

I. CLASSIFICATION/DECLASSIFICATION/MANDATORY REVIEW

A. TASK FORCE - Chairman -

DDO -
NFAC
DDS&T
DDA -
OGC -
IPS -

OS -
RAB -



STAT

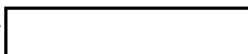
B. Approach - Will be to combine classification with declassification and develop common guidelines covering both aspects. To meet known requirements of the new E.O. both classified and unclassified guidelines will have to be developed. Since the system established for the development and approval of the current Agency declassification guidelines is still in existence, it is planned that this same system will be used to obtain overall coordination and approval for all guidelines that will be developed. Applicable regulations will be written/rewritten.

C. Problems - No specific problems have been identified.

D. Time Frame - In-house guidelines and regulations should be ready for formal coordination and approval by 1 October 1978. This will allow two months to complete this process so that they will be ready for use by the Agency on 1 December 1978. Unclassified guidelines for outside approval and publication in the Federal Register must be completed by 1 June 1979.

II. MARKINGS

A. TASK FORCE - Chairman -



STAT

STAT

DDO -
NFAC
DDS&T
DDA -
CGC -
OS -
RAB -



B. Approach - All classification markings and controls now in use throughout the Agency will have to be reviewed in light of the implementing order for the new E.O. to determine what changes will be required and how these changes should be implemented. Initial requirement will be to get OGC guidance on what markings and controls the implementing order for the new E.O. will probably allow so preliminary work can start as soon as possible. Applicable regulations will be written/rewritten.

The initial instructions and procedures dealing with markings will have to be followed by a detailed handbook on how these general procedures are to work, i.e., size and position of markings.

C. Problems - It is anticipated that due to the great number of individual interests involved in this general area a significant number of problems may be encountered.

D. Time Frame - All proposals ready for formal coordination and approval by 1 October 1978. All newly required stamps ready for distribution by 1 November 1978.

III. TRAINING

A. TASK FORCE - Chairman

OGC
RAB
OS -
OTR



STAT

B. Approach - Identify those elements that the new E.O. requires must be addressed and work with OTR to develop the most effective means of getting required information to all levels of the Agency. Special emphasis should be placed on determining whether an audio-visual presentation would be the most effective way to inform all Agency personnel on the changes the new E.O. brings to the current classification process. Applicable regulations will be written/rewritten.

C. Problems - No special problems have been identified as of this time.

D. Time Frame - Programs and procedures ready for in-house formal approvals by 1 October 1978. Actual training of employees to start by 1 November 1978.

IV. SAFEGUARDING

A. TASK FORCE - Chairman

DDA -
DDO -
DDS&T
NFAC
OGC -
OS -



STAT

B. Approach - Identify those elements of the new E.O. relating to the safeguarding of classified material that require implementation through revision of Agency regulations. The Office of Security has been preparing revised security regulations which will serve as a take-off point for the changes necessitated by the E.O. Specifically, the new regulations will replace the extant HR [redacted]

STAT

C. Problems - The principal problem associated with the implementation of safeguarding policy is caused by the fact that Headquarters Regulations depend largely on the development of the implementation directive for E.O. 12065. As a result, the promulgation of the implementing directive will be the pacing item.

D. Time Frame - Initial drafts on which to build the revised Headquarters Regulations are already available. They will be modified to be consistent with the implementing directive as it is developed. Assuming promulgation of the implementing directive by 30 September, final drafts of the Headquarters Regulations should be submitted to the Regulations Control Branch by 31 October.

V. APPROVALS/ACTION REQUIRED

1. Approval of the attached Headquarters Notice describing what is being done within the Agency to prepare for the implementation of the new E.O.

2. Approval for the use of senior Directorate Declassification Focal Point Officers and supporting structures in implementing the new E.O.

3. Appointment of representatives to the various task forces and agreement that additional personnel will be made available if required.

4. Coordination and approval of the final implementation package will be handled within the respective Directorates and independent offices by the below listed signatories.

APPROVED:

STAT

[Redacted Signature Box]

Michael J. Malanick
Directorate of Administration

26 July 1978
Date

STAT

[Redacted Signature Box]

Eloise Page
Directorate of Operations

26 July 78
Date

STAT

[Redacted Signature Box]

Ernest J. Zellmer
Directorate of Science and Technology

26 July 78
Date

STAT

[Redacted Signature Box]

Paul Walsh
National Foreign Assessment Center

7-26-78
Date

STAT

[Redacted Signature Box]

Office of General Counsel

7-26-78
Date

STAT

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300030001-3

Next 4 Page(s) In Document Exempt

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300030001-3

CLASSIFICATION GUIDES

ALTERNATIVE #1

Agency-wide guide.
Directorate guides.
Office guides.

Agency-wide guide would cover general type information common to all offices within the Agency.

Directorate guides would cover information unique to each directorate but common to all offices within each directorate.

Office guides would cover information unique to each office.

Agency-wide guide should be prepared by representatives from each directorate and approved by DCI.

Directorate guides should be prepared by representatives from each office within the directorate and approved by DD's.

Office guides should be prepared by representatives from each branch/section within office and approved by office head.

Decentralized system, but one office (AI/DDA?) should act as focal point and liaison between directorates.

Each office would have to work from three guides, but would not be burdened by unnecessary information.

ALTERNATIVE #2

Agency-wide guide.
Office guides.

Agency-wide guide would cover general type information common to all offices within the Agency.

Office guides would cover information unique to each office, but also information common within each directorate.

Agency-wide guide should be prepared by representatives from each directorate and approved by DCI.

Office guides should be prepared by representatives from each branch/section within office and approved by one person within each directorate (DD's?) to ensure consistency between offices in duplicative information.

One office (AI/DDA?) should act as focal point and liaison between directorates.

Each office would have two guides to work from, but duplication would exist between office guides.

ALTERNATIVE #3

Directorate guides.

Each directorate would have only one guide to cover both common type information and unique information within directorate/offices.

One person in Agency would act as coordinator and also approve each guide to ensure consistency between directorates.

Each office would have only one guide to work from, but would be burdened with unnecessary information.

Duplication would exist between guides.

ALTERNATIVE #4

Directorate guides.

Office guides.

Directorate guides would cover common-type information found within Agency, and information unique to each directorate but common to all offices within each directorate.

Office guides would cover information unique to each office.

Directorate guides should be coordinated and approved by one person to ensure consistency in duplicative information.

Office guides should be approved by office heads (or DD's?).

One office (AI/DDA?) should act as focal point.

Offices would have to work from two guides, but would not be burdened by unnecessary information.

Duplication would exist between directorate guides.

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300030001-3

Comments
alternative language
succinct justification

INFORMATION SECURITY OVERSIGHT OFFICE

COMPARISON OF MAJOR FEATURES OF
EXECUTIVE ORDERS GOVERNING THE
INFORMATION SECURITY PROGRAM

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300030001-3

I. CLASSIFICATION LEVELS

E.O. 10501, AS AMENDED	E. O. 11652	E. O. 12065	CURRENT DRAFT
<p>THREE LEVELS:</p> <p>TOP SECRET(TS)-EXCEPTIONALLY GRAVE DAMAGE</p> <p>SECRET(S)-SERIOUS DAMAGE</p> <p>CONFIDENTIAL(C)-PREJUDICIAL TO DEFENSE</p>	<p>THREE LEVELS:</p> <p>TS-EXCEPTIONALLY GRAVE DAMAGE</p> <p>S-SERIOUS DAMAGE</p> <p>C-DAMAGE</p>	<p>THREE LEVELS:</p> <p>TS-EXCEPTIONALLY GRAVE DAMAGE</p> <p>S-SERIOUS DAMAGE</p> <p>C-IDENTIFIABLE DAMAGE</p>	<p>THREE LEVELS:</p> <p>TS-EXCEPTIONALLY GRAVE DAMAGE</p> <p>S-SERIOUS DAMAGE</p> <p>C-DAMAGE</p>

COMMENT: THE TERM "IDENTIFIABLE" HAS BEEN OMITTED IN THE DRAFT ORDER TO OVERCOME LITIGATION PROBLEMS CONCERNING THE INTENT OF THE LANGUAGE OF E.O. 12065. IT IS NOT INTENDED NOR DOES EXPERIENCE INDICATE THAT ITS OMISSION WILL RESULT IN INFORMATION BEING CLASSIFIED UNDER THE DRAFT ORDER WHICH WOULD NOT BE CLASSIFIABLE UNDER E.O. 12065.

II. WHO MAY ORIGINALLY CLASSIFY

E.O. 10501, AS AMENDED	E.O. 11652	E.O. 12065	CURRENT DRAFT
<p>TOP SECRET: 48 AGENCIES -7,136 PERSONS SECRET: 48 AGENCIES -23,236 PERSONS CONFIDENTIAL: 48 AGENCIES -28,944 PERSONS</p> <p>TOTAL ORIGINAL CLASSIFIERS: 59,316</p> <p>NOTE: AGENCY AUTHORITY CITED ON THIS PAGE IS CUMULATIVE: I.E., AGENCIES WITH SECRET AUTHORITY INCLUDE THOSE WITH TOP SECRET. THE SAME APPLIES FOR CONFIDENTIAL.</p>	<p>TOP SECRET: 17 AGENCIES -1597 PERSONS SECRET: 30 AGENCIES -9986 PERSONS CONFIDENTIAL: 30 AGENCIES -6043 PERSONS</p> <p>TOTAL ORIGINAL CLASSIFIERS: 17,626</p>	<p>TOP SECRET: 13 AGENCIES -1496 PERSONS SECRET: 17 AGENCIES -4195 PERSONS CONFIDENTIAL: 19 AGENCIES -1538 PERSONS</p> <p>TOTAL ORIGINAL CLASSIFIERS: 7229</p>	<p>THE CURRENT DRAFT DOES NOT LIST THE AGENCIES WITH CLASSIFICATION AUTHORITY. THIS WILL BE ACCOMPLISHED BY AN ACCOMPANYING PRESIDENTIAL ORDER. PRESENT PLANS ANTICIPATE NUMBERS COMPARABLE TO E.O. 12065 IN BOTH NUMBERS OF AGENCIES AND PERSONNEL.</p>

COMMENT: THE CURRENT DRAFT REFLECTS COMMITMENT TO KEEP THE NUMBER OF CLASSIFIERS TO A NECESSARY MINIMUM, WHILE PROVIDING AN ADMINISTRATIVE REMEDY TO AVOID THE UNNECESSARY INVOLVEMENT OF THE HEAD OF THE AGENCY IN THE DELEGATION PROCESS.

III. CLASSIFICATION CATEGORIES

E.O. 10501, AS AMENDED	E.O. 11652	E.O. 12065	CURRENT DRAFT
NO SPECIFIC CATEGORIES ARE GIVEN WHICH LIMIT SUBJECT MATTERS THAT MAY BE CLASSIFIED	NO SPECIFIC CATEGORIES ARE GIVEN WHICH LIMIT SUBJECT MATTERS THAT MAY BE CLASSIFIED	<p>SEVEN CATEGORIES:</p> <ol style="list-style-type: none"> 1. MILITARY PLANS, WEAPONS, OR OPERATIONS; 2. FOREIGN GOVERNMENT INFORMATION; 3. INTELLIGENCE ACTIVITIES, SOURCES OR METHODS; 4. FOREIGN RELATIONS OR FOREIGN ACTIVITIES OF THE UNITED STATES; 5. SCIENTIFIC, TECHNOLOGICAL, OR ECONOMIC MATTERS RELATING TO THE NATIONAL SECURITY; 6. UNITED STATES GOVERNMENT PROGRAMS FOR SAFEGUARDING NUCLEAR MATERIALS OR FACILITIES; OR 7. OTHER CATEGORIES OF INFORMATION WHICH ARE RELATED TO NATIONAL SECURITY AND WHICH REQUIRE PROTECTION AGAINST UNAUTHORIZED DISCLOSURE AS DETERMINED BY THE PRESIDENT, BY A PERSON DESIGNATED BY THE PRESIDENT PURSUANT TO SEC. 1-201, OR BY AN AGENCY HEAD. 	<p>TEN CATEGORIES:</p> <ol style="list-style-type: none"> 1. MILITARY PLANS, WEAPONS, OR OPERATIONS; 2. THE VULNERABILITIES OR CAPABILITIES OF SYSTEMS, INSTALLATIONS, PROJECTS, OR PLANS VITAL TO THE NATIONAL SECURITY; 3. FOREIGN GOVERNMENT INFORMATION; 4. INTELLIGENCE ACTIVITIES (INCLUDING SPECIAL ACTIVITIES), OR INTELLIGENCE SOURCES OR METHODS; 5. FOREIGN RELATIONS OR FOREIGN ACTIVITIES OF THE UNITED STATES; 6. SCIENTIFIC, TECHNOLOGICAL, OR ECONOMIC MATTERS RELATING TO THE NATIONAL SECURITY; 7. UNITED STATES GOVERNMENT PROGRAMS FOR SAFEGUARDING NUCLEAR MATERIALS OR FACILITIES; 8. CRYPTOLOGY; 9. A CONFIDENTIAL SOURCE; OR 10. OTHER CATEGORIES OF INFORMATION WHICH ARE RELATED TO THE NATIONAL SECURITY AND WHICH REQUIRE PROTECTION AGAINST UNAUTHORIZED DISCLOSURE AS DETERMINED BY THE PRESIDENT OR BY AGENCY HEADS WHO HAVE ORIGINAL CLASSIFICATION AUTHORITY. ANY DETERMINATION MADE UNDER THIS SUBSECTION SHALL BE REPORTED PROMPTLY TO THE DIRECTOR OF THE INFORMATION SECURITY OVERSIGHT OFFICE.
<p>COMMENT: THE THREE ADDITIONAL CATEGORIES ADDED TO THE CURRENT DRAFT REFLECT EXPERIENCE OF 3 YEARS UNDER E.O. 12065 WHICH INDICATED THAT THE ELEMENTS ADDED WERE JEOPARDIZED IN THE CONTEXT OF LITIGATION. IT IS NOT INTENDED THAT ADDITIONAL MATERIAL WILL BE CLASSIFIED UNDER THESE CATEGORIES BEYOND THAT WHICH WAS SUBJECT TO CLASSIFICATION UNDER E.O. 12065.</p>			

IV. DURATION OF CLASSIFICATION

E.O. 10501, AS AMENDED	E.O. 11652	E.O. 12065	CURRENT DRAFT
<p>FOUR GROUPS:</p> <p>GROUP 1-NO LIMITATIONS ON DURATION</p> <p>GROUP 2-NO LIMITATIONS ON DURATION</p> <p>GROUP 3-NO LIMITATIONS ON DURATION</p> <p>GROUP 4-12 YEARS</p>	<p>THREE GROUPS:</p> <p>1. ADVANCED DECLASSIFICATION SCHEDULE- (ADS):</p> <p>TS-SOONER THAN 10 YEARS</p> <p>S-SOONER THAN 8 YEARS</p> <p>C-SOONER THAN 6 YEARS</p> <p>2. GENERAL DECLASSIFICATION SCHEDULE (GDS):</p> <p>TS-10 YEARS</p> <p>S-8 YEARS</p> <p>C-6 YEARS</p> <p>3. EXTENDED DECLASSIFICATION SCHEDULE: (XDS):</p> <p>TS-30 YEARS UNLESS EXTENDED</p> <p>S-30 YEARS UNLESS EXTENDED</p> <p>C-30 YEARS UNLESS EXTENDED</p>	<p>SIX YEARS UNLESS EXTENDED BY HEAD OF AGENCY OR TOP SECRET AUTHORITY FOR PERIODS UP TO 20 YEARS. FOLLOWING REVIEW, HEAD OF AGENCY MAY EXTEND BEYOND 20 YEARS.</p> <p>EXPERIENCE HAS SHOWN THAT THE OVERWHELMING MAJORITY (IN EXCESS OF 90%) NOT MARKED FOR AUTOMATIC DECLASSIFICATION IN SIX YEARS.</p>	<p>IF APPROPRIATE, A LIMIT SHALL BE ESTABLISHED AT TIME OF ORIGINAL CLASSIFICATION. CLASSIFICATION SHALL CONTINUE AS LONG AS REQUIRED BY NATIONAL SECURITY INTEREST.</p>

COMMENT: THE DRAFT ORDER RECOGNIZES THAT AUTOMATIC DECLASSIFICATION DATES WHICH DO NOT RELATE TO A SPECIFIC OCCURRENCE ARE ARTIFICIAL DETERMINATIONS WHICH POSE A THREAT TO SECURITY OF THE INFORMATION. EXPERIENCE INDICATES THAT AGENCIES AVOID AFFIXING AUTOMATIC DECLASSIFICATION DATES WHENEVER POSSIBLE.

V. LIMITATIONS ON CLASSIFICATION

E. O. 10501, as amended	E. O. 11652	E. O. 12065	Current draft
NO SPECIFIC GROUP OF LIMITATIONS. SOME REFERENCES TO AVOIDING UNNECESSARY OR INAPPROPRIATE CLASSIFICATION.	CLASSIFICATION SOLELY ON BASIS OF NATIONAL SECURITY CONSIDERATIONS. NOT TO CONCEAL INEFFICIENCY OR ERROR, TO PREVENT EMBARRASSMENT, TO RESTRAIN COMPETITION OR TO PREVENT THE RELEASE OF MATERIAL NOT REQUIRING NATIONAL SECURITY PROTECTION.	CLASSIFICATION IMPROPER WHEN USED TO CONCEAL VIOLATIONS OF LAW, INEFFICIENCY OR ERROR, PREVENT EMBARRASSMENT, OR RESTRAIN COMPETITION, OR LIMIT DISSEMINATION OF INFORMATION. BASIC SCIENTIFIC RESEARCH NOT CLEARLY RELATED TO NATIONAL SECURITY MAY NOT BE CLASSIFIED. CLASSIFICATION MAY NOT BE RESTORED TO DOCUMENTS DECLASSIFIED AND RELEASED TO THE PUBLIC, UNDER VERY LIMITED CIRCUMSTANCES DOCUMENTS CAN BE CLASSIFIED AFTER RECEIPT OF FOIA OR MANDATORY REVIEW REQUEST.	CLASSIFICATION SOLELY ON BASIS OF NATIONAL SECURITY CONSIDERATIONS. NOT TO CONCEAL VIOLATIONS OF LAW, INEFFICIENCY OR ERROR, PREVENT EMBARRASSMENT, RESTRAIN COMPETITION, OR DELAY RELEASE OF INFORMATION. UNDER VERY LIMITED CIRCUMSTANCES, DECLASSIFIED INFORMATION WHICH REQUIRES PROTECTION MAY BE RECLASSIFIED. UNDER LIMITED CIRCUMSTANCES, DOCUMENTS CAN BE CLASSIFIED AFTER RECEIPT OF FOIA OR MANDATORY REVIEW REQUEST.

COMMENTS: THE CURRENT DRAFT RETAINS THE CRITICAL LIMITATIONS OF THE EXISTING ORDER, IN ALLOWING THE VERY LIMITED RECLASSIFICATION OF MATERIAL PREVIOUSLY RELEASED, THE DRAFT RECOGNIZES INSTANCES IN WHICH THIS ACTION IS BOTH NECESSARY AND EFFECTIVE.

VI. RECOGNITION OF DERIVATIVE CLASSIFICATION

E. O. 10501, as amended	E. O. 11652	E. O. 12065	Current draft
NO RECOGNITION OF DISTINCTION BETWEEN ORIGINAL AND DERIVATIVE CLASSIFICATION.	NO SPECIFIC RECOGNITION OF DISTINCTION BETWEEN ORIGINAL AND DERIVATIVE CLASSIFICATION. HOLDERS OF CLASSIFIED INFORMATION ARE REQUIRED "TO OBSERVE AND RESPECT" THE CLASSIFICATION ASSIGNED BY THE ORIGINATOR.	RECOGNIZES DERIVATIVE CLASSIFICATION AS A COMPLETELY DISTINCT PROCESS FROM ORIGINAL CLASSIFICATION, BUT DOES NOT DEFINE DERIVATIVE CLASSIFICATION. ANY AUTHORIZED HOLDER OF CLASSIFIED INFORMATION MAY DERIVATIVELY CLASSIFY, EVEN PERSONS WITHOUT ORIGINAL CLASSIFICATION AUTHORITY. MANDATES CREATION OF CLASSIFICATION GUIDES TO BE USED BY DERIVATIVE CLASSIFIERS.	RECOGNIZES DERIVATIVE CLASSIFICATION AS A COMPLETELY DISTINCT PROCESS FROM ORIGINAL CLASSIFICATION, AND DEFINES THE TERM. ANY AUTHORIZED HOLDER OF CLASSIFIED INFORMATION MAY DERIVATIVELY CLASSIFY, EVEN PERSONS WITHOUT ORIGINAL CLASSIFICATION AUTHORITY. MANDATES CREATION OF CLASSIFICATION GUIDES, BUT AGENCY HEAD MAY WAIVE REQUIREMENT FOR SPECIFIC CLASSES OF INFORMATION AND REPORT WAIVER TO ISOO.

COMMENTS: ISOO EXPERIENCE IN MONITORING THE PROGRAM SHOWS THAT APPROXIMATELY 95% OF ALL CLASSIFICATION ACTIONS ARE DERIVATIVE IN NATURE, APPROPRIATE APPLICATION OF DERIVATIVE CLASSIFICATION PROMOTES UNIFORM CLASSIFICATION OF LIKE INFORMATION AND FACILITATES ITS SAFEGUARDING AND ULTIMATE DECLASSIFICATION. THE DRAFT ORDER REFLECTS ISOO EXPERIENCE THAT THERE ARE CERTAIN CLASSES OF INFORMATION FOR WHICH CLASSIFICATION GUIDES ARE INEFFECTUAL.

VII. AUTHORITY TO DECLASSIFY AND DOWNGRADE

E.O. 10501, AS AMENDED	E.O. 11652	E.O. 12065	CURRENT DRAFT
<p>HEAD OF AGENCY AND DESIGNEES MAY DECLASSIFY OR DOWNGRADE INFORMATION ORIGINATED WITHIN THAT AGENCY. HEAD OF AGENCY AND DESIGNEES MAY DECLASSIFY OR DOWNGRADE INFORMATION ORIGINATING IN ANOTHER AGENCY BUT IN THEIR POSSESSION BASED ON REGULATIONS ISSUED BY ORIGINATING AGENCY.</p>	<p>AUTHORITY TO DECLASSIFY OR DOWNGRADE RESTS WITH THE ORIGINATING OFFICIAL; A SUCCESSOR IN FUNCTION; A SUPERVISORY OFFICIAL OF EITHER; AND ANY OTHER OFFICIAL WITH TOP SECRET OR SECRET CLASSIFICATION AUTHORITY WHO HAS BEEN DESIGNATED BY ONE OF THE PRIOR LISTED OFFICIALS.</p>	<p>AUTHORITY TO DECLASSIFY OR DOWNGRADE RESTS WITH THE ORIGINATING OFFICIAL; A SUCCESSOR IN FUNCTION; A SUPERVISORY OFFICIAL OF EITHER; OR OTHER OFFICIALS DESIGNATED BY THE AGENCY HEAD. THE DIRECTOR OF ISOO MAY ORDER AN AGENCY HEAD TO DECLASSIFY INFORMATION DETERMINED TO BE CLASSIFIED IN VIOLATION OF THE ORDER. SUCH AN ORDER MAY BE APPEALED BY AGENCY HEAD TO NATIONAL SECURITY COUNCIL.</p>	<p>AUTHORITY TO DECLASSIFY OR DOWNGRADE RESTS WITH THE ORIGINATING OFFICIAL; A SUCCESSOR IN FUNCTION; A SUPERVISORY OFFICIAL OF EITHER; OR OTHER OFFICIALS DESIGNATED BY THE AGENCY HEAD OR THE SENIOR INFORMATION SECURITY PROGRAM OFFICIAL.</p>

COMMENT: THE DRAFT ORDER RETAINS THE DECLASSIFICATION PROCEDURES OF E.O. 12065 AS THEY PERTAIN TO AUTHORITY AND FACILITATES THE DECLASSIFICATION PROCESS BY ALLOWING THE AGENCY SENIOR OFFICIAL TO DESIGNATE DECLASSIFICATION AUTHORITIES.

VIII. SYSTEMATIC REVIEW

E. O. 10501, as amended	E. O. 11652	E. O. 12065	Current draft
NO PROVISIONS FOR SYSTEMATIC REVIEW.	ALL INFORMATION CLASSIFIED UNDER PRIOR ORDERS TO BE REVIEWED FOR DECLASSIFICATION BY THE ARCHIVIST OF THE UNITED STATES 30 YEARS FROM DATE OF ORIGIN. AGENCIES TO PROVIDE THE ARCHIVIST WITH GUIDELINES AND SUPPORT AS NEEDED. CLASSIFICATION OF SPECIFIC CATEGORIES OF INFORMATION MAY BE EXTENDED BEYOND 30 YEARS BY THE HEAD OF THE ORIGINATING AGENCY.	PERMANENTLY VALUABLE CLASSIFIED RECORDS SHALL BE SYSTEMATICALLY REVIEWED FOR DECLASSIFICATION TWENTY YEARS FROM DATE OF ORIGIN. AGENCY HEAD MAY EXTEND DECLASSIFICATION IN TEN YEAR INCREMENTS FOLLOWING REVIEW. FOREIGN GOVERNMENT INFORMATION TO BE REVIEWED 30 YEARS FROM DATE OF ORIGIN. ALL AGENCIES SHALL DEVELOP GUIDELINES FOR USE IN THIS PROGRAM.	SYSTEMATIC REVIEW TO BE CARRIED OUT BY THE ARCHIVIST, CONSISTENT WITH PROCEDURES PRESCRIBED BY ISOO AND AGENCY GUIDELINES, ON ALL MATERIAL ACCESSIONED INTO THE NATIONAL ARCHIVES AND CLASSIFIED PRESIDENTIAL PAPERS IN THE ARCHIVIST'S CONTROL. TIME-FRAMES TO BE ESTABLISHED IN ACCORDANCE WITH ISOO DIRECTIVES AND AGENCY GUIDELINES. AGENCY HEADS MAY CONDUCT SYSTEMATIC REVIEW PROGRAM ON PERMANENTLY VALUABLE RECORDS ORIGINATING IN THOSE AGENCIES.

COMMENTS: THE CURRENT DRAFT REPRESENTS A COMPROMISE POSITION BETWEEN THE RECOMMENDATION OF THE GENERAL ACCOUNTING OFFICE THAT SYSTEMATIC REVIEW BE ABOLISHED ENTIRELY AND THE CURRENT SYSTEM WHICH IS BOTH COSTLY AND UNSUCCESSFUL IN MEETING THE REQUIREMENTS OF THE ORDER. THE MORE REALISTIC PROGRAM ENVISIONED UNDER THE DRAFT ORDER WILL BETTER BALANCE THE NEEDS OF RESEARCHERS WITH AVAILABLE RESOURCES.

IX. MANDATORY REVIEW

E.O. 10501, AS AMENDED	E.O. 11652	E.O. 12065	CURRENT DRAFT
NO PROVISION REGARDING MANDATORY REVIEW.	ORIGINATOR SHALL REVIEW INFORMATION FOR POSSIBLE DECLASSIFICATION UPON A REQUEST BY AN AGENCY OR MEMBER OF THE GENERAL PUBLIC IF THE INFORMATION IS AT LEAST TEN YEARS OLD.	<p>A MEMBER OF THE PUBLIC OR GOVERNMENT AGENCY MAY, AT ANY TIME, REQUEST THAT CLASSIFIED INFORMATION BE REVIEWED FOR DECLASSIFICATION AND RELEASE. PRESIDENTIAL MATERIALS LESS THAN TEN YEARS OLD ARE EXEMPT FROM THIS REQUIREMENT. AGENCIES CANNOT REFUSE TO CONFIRM OR DENY THE EXISTENCE OF A DOCUMENT UNLESS THAT FACT IS CLASSIFIABLE UNDER THIS ORDER.</p> <p>IN MAKING DECLASSIFICATION DECISIONS THE ORIGINATOR SHOULD BALANCE THE BENEFITS TO THE PUBLIC FROM RELEASE OF INFORMATION AGAINST NATIONAL SECURITY CONSIDERATIONS.</p>	ALL INFORMATION SUBJECT TO MANDATORY REVIEW AT ANY TIME UPON REQUEST BY US CITIZEN, RESIDENT ALIEN, OR STATE OR LOCAL GOVERNMENT, REQUEST MUST BE SPECIFIC ENOUGH THAT AGENCIES CAN LOCATE THE INFORMATION WITH REASONABLE EFFORT. PRESIDENTIAL MATERIALS ARE SUBJECT TO MANDATORY REVIEW 12 YEARS AFTER CREATION. AGENCIES SHALL DEVELOP PROCEDURES FOR MANDATORY REVIEW, TO INCLUDE A METHOD OF APPEAL. INFORMATION SHALL BE REVIEWED BY THE ORIGINATOR IF IN THE CUSTODY OF ANOTHER AGENCY.

COMMENT: OMISSION OF THE "BALANCING TEST" IS DESIGNED TO PREVENT THE UNINTENDED JUDICIAL REVIEW OF EXECUTIVE BRANCH DISCRETION. BALANCING IS INHERENTLY A PART OF THE DECISION TO CLASSIFY AND DECLASSIFY INFORMATION. THE DELAY TO 12 YEARS FOR REVIEW OF PRESIDENTIAL RECORDS IS DESIGNED TO BE CONSISTENT WITH THE PRESIDENTIAL RECORDS ACT OF 1978.

X. SAFEGUARDING

E. O. 10501, as amended	E. O. 11652	E. O. 12065	Current draft
<p>SETS FORTH BASIC POLICIES CONCERNING ACCESS, STORAGE, LOCKS AND SECURITY CONTAINERS, DISSEMINATION, LOSS, COMPROMISE, ACCOUNTABILITY, TRANSMISSION, DESTRUCTION, ETC.</p>	<p>PROVIDED ESSENTIALLY THE SAME BASIC POLICIES FOR THE PROTECTION OF NATIONAL SECURITY INFORMATION. IN ADDITION, REQUIRED THE NATIONAL SECURITY COUNCIL TO ISSUE DIRECTIVES CONCERNING PROTECTION BASED ON THESE POLICIES.</p>	<p>IN ADDITION TO THE BASIC POLICIES SET FORTH IN PREDECESSOR ORDERS, INCLUDED DIRECTION FOR REPRODUCTION CONTROLS AND FOR MONITORSHIP OF SPECIAL ACCESS PROGRAMS BY THE DIRECTOR OF THE INFORMATION SECURITY OVERSIGHT OFFICE (ISOO). PROVIDES THAT THE ISOO PROMULGATE IMPLEMENTING SAFEGUARDING DIRECTIVES,</p>	<p>RETAINS THE SAFEGUARDING POLICIES OF E. O. 12065 WITH THE EXCEPTION OF THOSE PORTIONS DEALING WITH REPRODUCTION CONTROLS. ADDS PROVISIONS PROHIBITTING DISTRIBUTION OR DISSEMINATION OF INFORMATION TO A THIRD AGENCY WITHOUT THE AGREEMENT OF THE ORIGINATING AGENCY.</p>

COMMENTS: THE THIRD-AGENCY RULE CURRENTLY CONTAINED IN THE ISOO DIRECTIVE HAS BEEN PLACED IN THE DRAFT ORDER. THE IMPLEMENTING DIRECTIVE WILL REQUIRE AGENCIES TO ESTABLISH APPROPRIATE REPRODUCTION CONTROLS.

XI. OVERSIGHT

E.O. 10501, AS AMENDED	E.O. 11652	E.O. 12065	CURRENT DRAFT
MADE NO PROVISIONS FOR OVERSIGHT BY AN INDEPENDENT BODY. EACH AGENCY WAS RESPONSIBLE FOR MONITORING ITS OWN PROGRAM. THE NATIONAL SECURITY COUNCIL (NSC) WAS RESPONSIBLE FOR CONDUCTING A CONTINUING REVIEW OF THE IMPLEMENTATION OF THE ORDER TO ENSURE THAT CLASSIFIED DEFENSE INFORMATION WAS PROPERLY SAFEGUARDED.	<p>ESTABLISHED A SEVEN MEMBER INTERAGENCY CLASSIFICATION REVIEW COMMITTEE (ICRC) TO ASSIST THE NSC IN MONITORING IMPLEMENTATION OF THE ORDER. THE ICRC WAS CHARGED SPECIFICALLY TO OVERSEE AGENCY ACTIONS, TO INCLUDE APPROVAL OF AGENCY IMPLEMENTING DIRECTIVES, AND TO RECEIVE AND TAKE ACTION ON SUGGESTIONS AND COMPLAINTS REGARDING THE PROGRAM FROM PERSONS WITHIN OR OUTSIDE THE GOVERNMENT.</p> <p>HEADS OF AGENCIES WERE CHARGED TO DESIGNATE A SENIOR OFFICIAL RESPONSIBLE FOR EFFECTIVE IMPLEMENTATION AND FOR ENSURING THAT AGENCY PERSONNEL WERE FAMILIAR WITH THE REQUIREMENTS OF THE ORDER.</p>	<p>ESTABLISHES A SEPARATE AND INDEPENDENT BODY, THE INFORMATION SECURITY OVERSIGHT OFFICE (ISOO), TO MONITOR THE PROGRAM. PROVIDES AUTHORITY FOR THE DIRECTOR, ISOO, TO OVERSEE AND ENSURE COMPLIANCE WITH THE ORDER THROUGH ON-SITE REVIEWS OF AGENCY PROGRAMS, AND REVIEW AND APPROVE AGENCY IMPLEMENTING REGULATIONS AND SYSTEMATIC REVIEW GUIDELINES. REQUIRES THE DIRECTOR TO REPORT ANNUALLY TO THE PRESIDENT ON THE STATUS OF IMPLEMENTATION OF THE ORDER. THE DIRECTOR, ISOO, IS GIVEN THE AUTHORITY TO DEVELOP AND PROMULGATE DIRECTIVES FOR IMPLEMENTING THE ORDER THAT ARE BINDING ON AGENCIES. OVERALL POLICY DIRECTION FOR THE PROGRAM IS PROVIDED BY THE NATIONAL SECURITY COUNCIL.</p>	<p>THE CURRENT DRAFT ESSENTIALLY RETAINS ALL AUTHORITY PROVIDED TO THE ISOO BY E.O. 12065. IN ADDITION IT PROVIDES THE DIRECTOR THE AUTHORITY TO PRESCRIBE GOVERNMENT-WIDE STANDARD SECURITY FORMS AND TO APPOINT MEMBERS OF THE ISOO STAFF.</p> <p>THE DRAFT CONTINUES TO PROVIDE THAT THE NSC SHALL PROVIDE OVERALL POLICY DIRECTION FOR THE PROGRAM.</p>

COMMENT: CURRENT DRAFT CONTINUES TO RECOGNIZE THE NEED FOR AN INDEPENDENT OVERSIGHT ORGANIZATION.

XII. SANCTIONS

E. O. 10501, as amended	E. O. 11652	E. O. 12065	Current draft
<p>PROVIDED FOR NO SPECIFIC SANCTIONS EXCEPT THAT AGENCY HEADS WERE DIRECTED TO TAKE PROMPT AND STRINGENT ACTION AGAINST ANY EMPLOYEE DETERMINED TO HAVE BEEN KNOWINGLY RESPONSIBLE FOR THE UNAUTHORIZED RELEASE OR DISCLOSURE OF CLASSIFIED DEFENSE INFORMATION.</p>	<p>SANCTIONS WERE LIMITED TO CASES OF REPEATED UNNECESSARY CLASSIFICATION OR OVERCLASSIFICATION AND TO UNAUTHORIZED DISCLOSURES OF NATIONAL SECURITY INFORMATION.</p>	<p>SANCTIONS WERE EXPANDED TO COVER KNOWING AND WILLFUL (1) CLASSIFICATION IN VIOLATION OF THE ORDER; (2) UNAUTHORIZED DISCLOSURE; OR (3) VIOLATION OF ANY OTHER PROVISION OF THE ORDER OR IMPLEMENTING DIRECTIVES. A RANGE OF SANCTIONS FROM REPRIMAND TO REMOVAL WAS ESTABLISHED. THE DIRECTOR OF ISOO MUST BE INFORMED OF ALL VIOLATIONS AND CORRECTIVE ACTIONS TAKEN.</p>	<p>THE SANCTION PROVISIONS OF E. O. 12065 ARE CONTINUED IN THE CURRENT DRAFT. THE ONE ADDITION IS PROVISION FOR "NEGLIGENT" UNAUTHORIZED DISCLOSURE OR "NEGLIGENT" VIOLATION OF ANY OTHER PROVISION OF THE ORDER OR IMPLEMENTING DIRECTIVES. THE RANGE OF SANCTIONS PROVIDED BY E. O. 12065 IS CONTINUED, AS WELL AS PROVISIONS FOR THE DIRECTOR, ISOO, TO BE NOTIFIED IN CASES OF UNAUTHORIZED DISCLOSURE OR CLASSIFICATION IN VIOLATION OF THE ORDER.</p>

COMMENTS: CURRENT DRAFT RETAINS AND STRENGTHENS THE SANCTION PROVISIONS OF E. O. 12065. IT RELIEVES THE REQUIREMENT THAT AGENCIES MAKE ON-THE-SPOT REPORTS OF MINOR ADMINISTRATIVE VIOLATIONS TO THE ISOO.

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>Executive Order 12065 June 26, 1978</p> <p>National Security Information</p> <p>By the authority vested in me as President by the Constitution and laws of the United States of America, in order to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure, it is hereby ordered as follows:</p> <p>TABLE OF CONTENTS</p> <p>Section 1. Original Classification: (FR prep)</p> <p>1-1 Classification Designation (20050)</p> <p>1-2 Classification Authority (20050)</p> <p>1-3 Classification Requirements (20051)</p> <p>1-4 Duration of Classification (20052)</p> <p>1-5 Identification and Markings (20053)</p> <p>1-6 Prohibitions (20053)</p> <p>Section 2. Derivative Classification:</p> <p>2-1 Use of Derivative Classification (20053)</p> <p>2-2 Classification Guides (20053)</p> <p>2-3 New Material (20054)</p> <p>Section 3. Declassification and Downgrading:</p> <p>3-1 Declassification Authority (20054)</p> <p>3-2 Transferred Information (20054)</p> <p>3-3 Declassification Policy (20055)</p> <p>3-4 Systematic Review for Declassification (20056)</p> <p>3-5 Mandatory Review for Declassification (20056)</p> <p>3-6 Downgrading (20057)</p> <p>Section 4. Safeguarding:</p> <p>4-1 General Restrictions (20057)</p> <p>4-2 Special Access Programs (20057)</p> <p>4-3 Access by Historical Researchers and Former Presidential Appointees (20058)</p> <p>4-4 Reproduction Controls (20058)</p> <p>Section 5. Information Security Review:</p> <p>5-1 Oversight (20059)</p> <p>5-2 Information Security Oversight Office (20059)</p> <p>5-3 Interagency Information Security Committee (20060)</p> <p>5-4 General Responsibilities (20060)</p> <p>5-5 Administrative Structures (20061)</p> <p>Section 6. General Provisions:</p> <p>6-1 Definitions (20061)</p> <p>6-2 General (20061)</p>	<p>Executive Order _____ Date _____</p> <p>National Security Information</p> <p>TABLE OF CONTENTS</p> <p>SECTION 1.1 ORIGINAL CLASSIFICATION:</p> <p>SEC 1.1 CLASSIFICATION LEVELS</p> <p>SEC 1.2 CLASSIFICATION AUTHORITY</p> <p>SEC 1.3 CLASSIFICATION CATEGORIES</p> <p>SEC 1.4 DURATION OF CLASSIFICATION</p> <p>SEC 1.5 IDENTIFICATION AND MARKINGS</p> <p>SEC 1.6 LIMITATION ON CLASSIFICATION</p> <p>PART 2. DERIVATIVE CLASSIFICATION:</p> <p>SEC 2.1 USE OF DERIVATIVE CLASSIFICATION</p> <p>SEC 2.2 CLASSIFICATION GUIDES</p> <p>PART 3. DECLASSIFICATION AND DOWNGRADING:</p> <p>SEC 3.1 DECLASSIFICATION AUTHORITY</p> <p>SEC 3.2 TRANSFERRED INFORMATION</p> <p>SEC 3.3 SYSTEMATIC REVIEW FOR DECLASSIFICATION</p> <p>SEC 3.4 MANDATORY REVIEW FOR DECLASSIFICATION</p> <p>PART 4. SAFEGUARDING:</p> <p>SEC 4.1 GENERAL RESTRICTIONS ON ACCESS</p> <p>SEC 4.2 SPECIAL ACCESS PROGRAMS</p> <p>SEC 4.3 ACCESS BY HISTORICAL RESEARCHERS AND FORMER PRESIDENTIAL APPOINTEES</p> <p>PART 5. IMPLEMENTATION AND REVIEW:</p> <p>SEC 5.1 POLICY DIRECTION</p> <p>SEC 5.2 INFORMATION SECURITY OVERSIGHT OFFICE</p> <p>SEC 5.3 GENERAL RESPONSIBILITIES</p> <p>SEC 5.4 SANCTIONS</p> <p>PART 6. GENERAL PROVISIONS:</p> <p>SEC 6.1 DEFINITIONS</p> <p>SEC 6.2 GENERAL</p>	

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

2

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>SECTION 1. ORIGINAL CLASSIFICATION.</p> <p>1-1. <u>Classification Designation.</u></p> <p>1-101. Except as provided in the Atomic Energy Act of 1954, as amended, this Order provides the only basis for classifying information. Information may be classified in one of the three designations listed below. If there is reasonable doubt which designation is appropriate, or whether the information should be classified at all, the less restrictive designation should be used, or the information should not be classified.</p> <p>1-102. "Top Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.</p> <p>1-103. "Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.</p> <p>1-104. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security.</p>	<p>EXECUTIVE ORDER _____</p> <p>NATIONAL SECURITY INFORMATION</p> <p>This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Nothing in this Order limits the protection afforded any information by other provisions of law.</p> <p>PART I</p> <p>ORIGINAL CLASSIFICATION</p> <p>SECTION 1.1 <u>Classification Levels.</u></p> <p>(a) National security information (hereinafter "classified information") shall be classified at one of the following three levels:</p> <p>(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.</p> <p>(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.</p> <p>(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.</p> <p>(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information.</p> <p>(c) If there is reasonable doubt either about the need to classify information or about which classification level is appropriate, the information shall be considered classified and shall be safeguarded as required for the higher level of classification under the provisions of this Order pending a final determination by an original classification authority.</p>	<p>Preamble: The draft preamble is designed to introduce the purpose and tone of the Order. It stresses a more even approach to the question of protection of information versus openness.</p> <p>Section 1.1 of the proposed Order has been rewritten to view classification in a positive rather than a negative light.</p> <p>Section 1.1(a)(3) of the proposed Order eliminates the word "Identifiable" to avoid litigation problems that may arise if a quantum standard is applied to this word.</p> <p>Section 1.1(c) of the proposed Order stresses the need to protect information that may be classified; it replaces the negative tone in the current order.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

3

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>1-2. <i>Classification Authority.</i></p> <p>1-201. <i>Top Secret.</i> Authority for original classification of information as Top Secret may be exercised only by the President, by such officials as the President may designate by publication in the <u>FEDERAL REGISTER</u>, by the agency heads listed below, and by officials to whom such authority is delegated in accordance with Section 1-204:</p> <ul style="list-style-type: none"> The Secretary of State The Secretary of the Treasury The Secretary of Defense The Secretary of the Army The Secretary of the Navy The Secretary of the Air Force The Attorney General The Secretary of Energy The Chairman, Nuclear Regulatory Commission The Director, Arms Control and Disarmament Agency The Director of Central Intelligence The Administrator, National Aeronautics and Space Administration The Administrator of General Services (delegable only to the Director, Federal Preparedness Agency and to the Director, Information Security Oversight Office) <p>1-202. <i>Secret.</i> Authority for original classification of information as Secret may be exercised only by such officials as the President may designate by publication in the <u>FEDERAL REGISTER</u>, by the agency heads listed below, by officials who have Top Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:</p> <ul style="list-style-type: none"> The Secretary of Commerce The Secretary of Transportation The Administrator, Agency for International Development The Director, International Communication Agency <p>1-203. <i>Confidential.</i> Authority for original classification of information as Confidential may be exercised only by such officials as the President may designate by publication in the <u>FEDERAL REGISTER</u>, by the agency heads listed below, by officials who have Top Secret or Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:</p> <ul style="list-style-type: none"> The President and Chairman, Export-Import Bank of the United States The President and Chief Executive Officer, Overseas Private Investment Corporation 	<p>SEC 1.2</p> <p><u>Classification Authority.</u></p> <p>(a) <u>Top Secret.</u> The authority to classify information originally as Top Secret may be exercised only by:</p> <ol style="list-style-type: none"> (1) the President; (2) agency heads and officials designated by the President in the <u>Federal Register</u>; and (3) officials delegated this authority under Section 1.2(d). <p>(b) <u>Secret.</u> The authority to classify information originally as Secret may be exercised only by:</p> <ol style="list-style-type: none"> (1) agency heads and officials designated by the President in the <u>Federal Register</u>; (2) officials with original Top Secret classification authority; and (3) officials delegated such authority pursuant to Section 1.2(d). <p>(c) <u>Confidential.</u> The authority to classify information originally as Confidential may be exercised only by:</p> <ol style="list-style-type: none"> (1) agency heads and officials designated by the President in the <u>Federal Register</u>; (2) officials with original Top Secret or Secret classification authority; and (3) officials delegated such authority pursuant to Section 1.2(d). 	<p>Sections 1.2(a) thru 1.2(c): The listing of classification officials in the present Order will be replaced by a separate listing outside the body of the Order. This is more practical from an administrative standpoint. The methods of delegation have been broken out in the draft for clarity.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

4

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>1-204. <i>Limitations on Delegation of Classification Authority.</i></p> <p>(a) Authority for original classification of information as Top Secret may be delegated only to principal subordinate officials who have a frequent need to exercise such authority as determined by the President or by agency heads listed in Section 1-201.</p> <p>(b) Authority for original classification of information as Secret may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201 and 1-202, and by officials with Top Secret classification authority.</p> <p>(c) Authority for original classification of information as Confidential may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201, 1-202, and 1-203, and by officials with Top Secret classification authority.</p> <p>(d) Delegated original classification authority may not be redelegated.</p> <p>(e) Each delegation of original classification authority shall be in writing by name or title of position held.</p> <p>(f) Delegations of original classification authority shall be held to an absolute minimum. Periodic reviews of such delegations shall be made to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.</p> <p>1-205. <i>Exceptional Cases.</i> When an employee or contractor of an agency that does not have original classification authority originates information believed to require classification, the information shall be protected in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly under appropriate safeguards to the agency which has appropriate subject matter interest and classification authority. That agency shall decide within 30 days whether to classify that information. If it is not clear which agency should get the information, it shall be sent to the Director of the Information Security Oversight Office established in Section 3-2 for a determination.</p>	<p>(d) <i>Delegation of Original Classification Authority.</i></p> <p>(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.</p> <p>(2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Top Secret classification authority by the agency head.</p> <p>(3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Secret classification authority by the agency head.</p> <p>(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Secret or Confidential classification authority by the agency head.</p> <p>(5) Each delegation of original classification authority shall be in writing and shall not be delegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.</p> <p>(e) <i>Exceptional Cases.</i> When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information to that agency for a classification determination.</p>	<p>Sections 1.2(i) of the proposed Order adds the senior official designated under Section 5.3(a)(1) of the draft to those able to delegate classification authority. This will reduce the administrative burden on agency heads. Other changes are editorial and improve clarity.</p> <p>Section 1.2(a) of the proposed Order extends the responsibility for protection of information to government licensees. This change eliminates the uncertainty of whether or not licensees are covered under the present order.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

5

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p><u>1-3. Classification Requirements.</u></p> <p>1-301. Information may not be considered for classification unless it concerns:</p> <ul style="list-style-type: none"> (a) military plans, weapons, or operations; (b) foreign government information; (c) intelligence activities, sources or methods; (d) foreign relations or foreign activities of the United States; (e) scientific, technological, or economic matters relating to the national security; (f) United States Government programs for safeguarding nuclear materials or facilities; or (g) other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President, by a person designated by the President pursuant to Section 1-201, or by an agency head. <p>1-302. Even though information is determined to concern one or more of the criteria in Section 1-301, it may not be classified unless an original classification authority also determines that its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security.</p> <p>1-303. Unauthorized disclosure of foreign government information or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security.</p> <p>1-304. Each determination under the criterion of Section 1-301(g) shall be reported promptly to the Director of the Information Security Oversight Office.</p>	<p>SEC 1.3 <u>Classification Categories.</u></p> <p>(a) Information shall be considered for classification if it concerns:</p> <ul style="list-style-type: none"> (1) military plans, weapons, or operations; (2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security; (3) foreign government information; (4) intelligence activities (including special activities), or intelligence sources or methods; (5) foreign relations or foreign activities of the United States; (6) scientific, technological, or economic matters relating to the national security; (7) United States Government programs for safeguarding nuclear materials or facilities; (8) cryptology; (9) a confidential source; or (10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office. <p>(b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.</p> <p>(c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.</p> <p>(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.</p>	<p>Section 1.3(a) of the proposed Order lists the additional categories (12),(18),(19), that have been added based on litigation experience under the Freedom of Information Act. The phrase "including special activities" in 1.3(a)(4) has been added to ensure that special intelligence activities receive protection under this order. All other changes are editorial.</p> <p>Section 1.3(b) of the proposed Order has added language to make clear that classification is proper in certain situations when information becomes sensitive in the context of other information. (The mosaic approach)</p> <p>Section 1.3(c) of the proposed Order adds intelligence sources and methods to emphasize their sensitivity.</p> <p>Section 1.3(d) of the proposed Order is added to prevent the use of inadvertent or unauthorized release of information as an argument for release in litigation.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

6

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p><u>1-4. Duration of Classification.</u></p> <p>1-401. Except as permitted in Section 1-402, at the time of the original classification each original classification authority shall set a date or event for automatic declassification no more than six years later.</p> <p>1-402. Only officials with Top Secret classification authority and agency heads listed in Section 1-2 may classify information for more than six years from the date of the original classification. This authority shall be used sparingly. In such cases, a declassification date or event, or a date for review, shall be set. This date or event shall be as early as national security permits and shall be no more than twenty years after original classification, except that for foreign government information the date or event may be up to thirty years after original classification.</p>	<p>SEC 1.4 <u>Duration of Classification.</u></p> <p>(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.</p> <p>(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.</p> <p>(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.</p>	<p>Section 1.4(a) of the proposed Order has been changed to reflect the realization that automatic declassification dates are artificial, dangerous, and do not appreciably result in greater release of information.</p>
<p><u>1-5. Identification and Markings.</u></p> <p>1-501. At the time of original classification, the following shall be shown on the face of paper copies of all classified documents:</p> <p>(a) the identity of the original classification authority;</p> <p>(b) the office of origin;</p> <p>(c) the date or event for declassification or review; and</p> <p>(d) one of the three classification designations defined in Section 1-1.</p>	<p>SEC 1.5 <u>Identification and Markings.</u></p> <p>(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:</p> <p>(1) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;</p> <p>(2) the agency and office of origin;</p> <p>(3) the date or event for declassification, or the notation "Originating Agency's Determination Required"; and</p> <p>(4) one of the three classification levels defined in Section 1.1.</p>	<p>Sections 1.4(b) and 1.4(c) of the proposed Order are needed to make classification decisions under prior orders valid under the draft order.</p> <p>Section 1.5(a)(1) and (2) of the proposed Order contain editorial changes.</p> <p>Section 1.5(a)(3) of the proposed Order prescribes a standard declassification marking for information whose declassification is not tied to a date or event.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

7

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>1-502. Documents classified for more than six years shall also be marked with the identity of the official who authorized the prolonged classification. Such documents shall be annotated with the reason the classification is expected to remain necessary, under the requirements of Section 1-3, despite the passage of time. The reason for the prolonged classification may be stated by reference to criteria set forth in agency implementing regulations. These criteria shall explain in narrative form the reason the information needs to be protected beyond six years. If the individual who signs or otherwise authenticates a document also is authorized to classify it, no further annotation of identity is required.</p> <p>1-503. In order to facilitate excerpting and other uses, each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification designation, and which portions are not classified. The Director of the Information Security Oversight Office may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information.</p> <p>1-503. Only the designations prescribed by this Order may be used to identify classified information. Markings such as "For Official Use Only" and "Limited Official Use" may not be used for that purpose. Terms such as "Conference" or "Agency" may not be used in conjunction with the classification designations prescribed by this Order; e.g., "Agency Confidential" or "Conference Confidential."</p> <p>1-505. Foreign government information shall either retain its original classification designation or be assigned a United States classification designation that shall ensure a degree of protection equivalent to that required by the entity that furnished the information.</p> <p>1-506. Classified documents that contain or reveal information that is subject to special dissemination and reproduction limitations authorized by this Order shall be marked clearly so as to place the user on notice of the restrictions.</p>	<p>(b) Each classified document transmitted outside the originating agency shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.</p> <p>(c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.</p> <p>(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.</p> <p>(e) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).</p>	<p>Section 1.5(b) of the proposed Order seeks to reduce the administrative burden on agencies by allowing agency heads, for good cause, to waive portion marking requirements.</p> <p>Section 1.5(c) of the proposed Order provides for central guidance to achieve consistency of markings.</p> <p>Section 1.5(a) of the proposed Order is added to ensure protection for information classified under predecessor orders but not fully marked with all markings required under proposed Order.</p> <p>Section 1-506 of the present Executive Order has been dropped as unnecessary.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

8

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>1-6. Prohibition.</p> <p>1-601. Classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.</p> <p>1-602. Basic scientific research information not clearly related to the national security may not be classified.</p> <p>1-603. A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under this Order until and unless the government acquires a proprietary interest in the product. This Order does not affect the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-189).</p> <p>1-604. References to classified documents that do not disclose classified information may not be classified or used as a basis for classification.</p> <p>1-605. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of this Order or to prevent or delay the public release of such information.</p> <p>1-606. No document originated on or after the effective date of this Order may be classified after an agency has received a request for the document under the Freedom of Information Act or the Mandatory Review provisions of this Order (Section 3-5), unless such classification is consistent with this Order and is authorized by the agency head or deputy agency head. Documents originated before the effective date of this Order and subject to such a request may not be classified unless such classification is consistent with this Order and is authorized by the senior official designated to oversee the agency information security program or by an official with Top Secret classification authority. Classification authority under this provision shall be exercised personally, on a document-by-document basis.</p> <p>1-607. Classification may not be restored to documents already declassified and released to the public under this Order or prior Orders.</p>	<p>SEC 1.6 <u>Limitations on Classification.</u></p> <p>(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.</p> <p>(b) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may re-classify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered.</p> <p>(c) Information may be classified or re-classified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1), or an official with original Top Secret classification authority.</p>	<p>Section 1.6(a) of the proposed Order contains editorial changes.</p> <p>Sections 1-602 thru 1-604 of the present Order have been dropped because they are self-evident.</p> <p>Section 1.6(b) of the proposed Order provides limited authority for re-classification of information requiring national security protection because of changing circumstances.</p> <p>Section 1.6(c) of the proposed Order lowers the level specified in Section 1-606 of the current Executive Order for classification of material after receipt of FOIA or mandatory review request. This change will reduce the administrative burden on agency heads.</p> <p>Section 1-607 of the present Order has been dropped. This change is a change in policy and is covered in Section 1.6(b) of the draft.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

9

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>SECTION 2. DERIVATIVE CLASSIFICATION.</p> <p>2-1. <i>Use of Derivative Classification.</i></p> <p>2-101. Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide.</p> <p>2-102. Persons who apply such derivative classification markings shall:</p> <p>(a) respect original classification decisions;</p> <p>(b) verify the information's current level of classification so far as practicable before applying the markings; and</p> <p>(c) carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings, in accordance with Sections 2-2 and 2-301 below. A single marking may be used for documents based on multiple sources.</p>	<p>PART 2</p> <p>DERIVATIVE CLASSIFICATION</p> <p>SEC 2.1 <u>Use of Derivative Classification.</u></p> <p>(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.</p> <p>(b) Persons who apply derivative classification markings shall:</p> <p>(1) observe and respect original classification decisions; and</p> <p>(2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.</p>	<p>Section 2.1 of the proposed Order contains editorial changes.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

10

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>2-2. <u>Classification Guides.</u></p> <p>2-201. Classification guides used to direct derivative classification shall specifically identify the information to be classified. Each classification guide shall specifically indicate how the designations, time limits, markings, and other requirements of this Order are to be applied to the information.</p> <p>2-202. Each such guide shall be approved personally and in writing by an agency head listed in Section 1-2 or by an official with Top Secret classification authority. Such approval constitutes an original classification decision.</p> <p>2-3. <u>New Material.</u></p> <p>2-301. New material that derives its classification from information classified on or after the effective date of this Order shall be marked with the declassification date or event, or the date for review, assigned to the source information.</p> <p>2-302. New material that derives its classification from information classified under prior Orders shall be treated as follows:</p> <p>(a) If the source material bears a declassification date or event twenty years or less from the date of origin, that date or event shall be carried forward on the new material.</p> <p>(b) If the source material bears no declassification date or event or is marked for declassification beyond twenty years, the new material shall be marked with a date for review for declassification at twenty years from the date of original classification of the source material.</p> <p>(c) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond thirty years, the new material shall be marked for review for declassification at thirty years from the date of original classification of the source material.</p>	<p>SEC 2.2 <u>Classification Guides.</u></p> <p>(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.</p> <p>(b) Each guide shall be approved personally and in writing by an official who:</p> <p>(1) has program or supervisory responsibility over the information or is the senior agency official designated under Section 5.3(a)(1); and</p> <p>(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.</p> <p>(c) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.</p>	<p>Section 2.2(a) of the proposed Order contains changes which clarify the purpose of classification guides and who is responsible for their preparation.</p> <p>Section 2.2(b) of the proposed Order has been changed to include the program manager and senior agency official as approving authorities for classification guides.</p> <p>Section 2.2(c) of the proposed Order has been added to give agencies more flexibility in determining their needs for classification guides.</p> <p>Section 2-3 of the present Order has been deleted. This section involves administrative requirements which will be addressed more properly in the implementing directive.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

11

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>SECTION 5. DECLASSIFICATION AND DOWNGRADING.</p> <p>5-1. <i>Declassification Authority.</i></p> <p>5-101. The authority to declassify or downgrade information classified under this or prior Orders shall be exercised only as specified in Section 5-1.</p> <p>5-102. Classified information may be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, by a successor, or by a supervisory official of either.</p> <p>5-103. Agency heads named in Section 5-2 shall designate additional officials at the lowest practicable echelons to exercise declassification and downgrading authority.</p> <p>5-104. If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first.</p> <p>5-105. The provisions of this Order relating to declassification shall also apply to agencies which, under the terms of this Order, do not have original classification authority but which had such authority under prior Orders.</p>	<p>PART 3</p> <p>DECLASSIFICATION AND DOWNGRADING</p> <p>SEC 3.1 <i>Declassification Authority.</i></p> <p>(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order.</p> <p>(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1).</p> <p>(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified until the appeal is decided.</p> <p>(d) The provisions of this Section shall apply to agencies that, under the terms of this Order, do not have original classification authority, but that had such authority under predecessor orders.</p>	<p>Section 3.1(a) of the proposed Order contains editorial changes.</p> <p>Section 3.1(b) of the proposed Order adds a senior agency official to the list of officials authorized to declassify or downgrade classified information.</p> <p>Section 3.1(c) of the proposed Order removes the one year deadline for a decision on appeals.</p> <p>Section 3.1(d) of the proposed Order contains editorial changes.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

12

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>3-2. Transferred Information.</p> <p>3-201. For classified information transferred in conjunction with a transfer of functions—not merely for storage purposes—the receiving agency shall be deemed to be the originating agency for all purposes under this Order.</p> <p>3-202. For classified information not transferred in accordance with Section 3-201, but originated in an agency which has ceased to exist, each agency in possession shall be deemed to be the originating agency for all purposes under this Order. Such information may be declassified or downgraded by the agency in possession after consulting with any other agency having an interest in the subject matter.</p> <p>3-203. Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and the agency guidelines.</p> <p>3-204. After the termination of a Presidential administration, the Archivist of the United States shall review and declassify or downgrade all information classified by the President, the White House Staff, committees or commissions appointed by the President, or others acting on the President's behalf. Such declassification shall only be undertaken in accordance with the provisions of Section 3-204.</p> <p>3-3. Declassification Policy.</p> <p>3-301. Declassification of classified information shall be given emphasis comparable to that accorded classification. Information classified pursuant to this and prior Orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event.</p> <p>3-302. When information is reviewed for declassification pursuant to this Order or the Freedom of Information Act, it shall be declassified unless the declassification authority established pursuant to Section 3-1 determines that the information continues to meet the classification requirements prescribed in Section 1-3 despite the passage of time.</p> <p>3-303. It is presumed that information which continues to meet the classification requirements in Section 1-3 requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head, a senior agency official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under this Order, an official with Top Secret classification authority, or the Archivist of the United States in the case of material covered in Section 3-203. That official will determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.</p>	<p>SEC 3.2 Transferred Information.</p> <p>(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.</p> <p>(b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.</p> <p>(c) Classified information transferred to the General Services Administration for accession into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.</p>	<p>Section 3.2(a) of the proposed Order contains editorial changes.</p> <p>Section 3.2(b) of the proposed Order contains editorial changes.</p> <p>Section 3.2(c) of the proposed Order contains no changes.</p> <p>Section 3-204 of the present Order is dropped because the subject is addressed in the Presidential Records Act of 1978 and Section 3.4(b) of the proposed Order.</p> <p>Section 3-301 of the present Order is dropped because the language is considered unnecessary. Also, a portion of this section is included in Section 3.1(a) of the proposed Order.</p> <p>Section 3-302 of the present Order is dropped because the language is considered unnecessary. Also, a portion of this section is included in Section 3.1(a) of the proposed Order.</p> <p>Section 3-303 of the present Order has been dropped because it has been incorrectly construed as a mechanism through which an individual could prevail upon the courts to gain access to properly classified information rather than a judgment to be applied at the sole discretion of the agency head as intended by the Order.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

13

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p><u>3-4. Systematic Review for Declassification.</u></p> <p>3-401. Classified information constituting permanently valuable records of the Government, as defined by 44 U.S.C. 2105, and information in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be reviewed for declassification as it becomes twenty years old. Agency heads listed in Section 1-2 and officials designated by the President pursuant to Section 1-201 of this Order may extend classification beyond twenty years, but only in accordance with Sections 3-3 and 3-402. This authority may not be delegated. When classification is extended beyond twenty years, a date no more than ten years later shall be set for declassification or for the next review. That date shall be marked on the document. Subsequent reviews for declassification shall be set at no more than ten year intervals. The Director of the Information Security Oversight Office may extend the period between subsequent reviews for specific categories of documents or information.</p> <p>3-402. Within 180 days after the effective date of this Order, the agency heads listed in Section 1-2 and the heads of agencies which had original classification authority under prior orders shall, after consultation with the Archivist of the United States and review by the Information Security Oversight Office, issue and maintain guidelines for systematic review covering twenty-year old classified information under their jurisdiction. These guidelines shall state specific, limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond twenty years is needed. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information. All information not identified in these guidelines as requiring review and for which a prior automatic declassification date has not been established shall be declassified automatically at the end of twenty years from the date of original classification.</p> <p>3-403. Notwithstanding Sections 3-401 and 3-402, the Secretary of Defense may establish special procedures for systematic review and declassification of classified cryptographic information, and the Director of Central Intelligence may establish special procedures for systematic review and declassification of classified information concerning the identities of clandestine human agents. These procedures shall be consistent, so far as practicable, with the objectives of Sections 3-401 and 3-402. Prior to implementation, they shall be reviewed and approved by the Director of the Information Security Oversight Office and, with respect to matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Disapproval of procedures by the Director of the Information Security Oversight Office may be appealed to the National Security Council. In such cases, the procedures shall not be implemented until the appeal is decided.</p> <p>3-404. Foreign government information shall be exempt from automatic declassification and twenty year systematic review. Unless declassified earlier, such information shall be reviewed for declassification thirty years from its date of origin. Such review shall be in accordance with the provisions of Section 3-3 and with guidelines developed by agency heads in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information.</p> <p>3-405. Transition to systematic review at twenty years shall be implemented as rapidly as practicable and shall be completed no more than ten years from the effective date of this Order.</p>	<p>3.3 <u>Systematic Review for Declassification</u></p> <p>(a) The Archivist of the United States shall, in accordance with procedures prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records in the Archivist's possession and control. Such information shall be reviewed by the Archivist for declassification in accordance with systematic review guidelines that shall be provided by agency heads who originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.</p> <p>(b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States.</p> <p>(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptographic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.</p>	<p>Section 3.3 The systematic review program of the present Order is not cost efficient. The proposed Order reflects economic realities. The only classified records that are required to be systematically reviewed under the proposed Order are those accessioned into the National Archives of the United States and classified Presidential papers or records in the Archivist's possession and control. Agency heads may conduct internal systematic review programs for classified information originated by them.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

14

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>3-5. <u>Mandatory Review for Declassification.</u></p> <p>3-501. Agencies shall establish a mandatory review procedure to handle requests by a member of the public, by a government employee, or by an agency, to declassify and release information. This procedure shall apply to information classified under this Order or prior Orders. Except as provided in Section 3-503, upon such a request the information shall be reviewed for possible declassification, provided the request reasonably describes the information. Requests for declassification under this provision shall be acted upon within 60 days. After review, the information or any reasonably segregable portion thereof that no longer requires protection under this Order shall be declassified and released unless withholding is otherwise warranted under applicable law.</p> <p>3-503. Information less than ten years old which was originated by the President, by the White House Staff, or by committees or commissions appointed by the President, or by others acting on behalf of the President, including such information in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107 note, is exempted from the provisions of Section 3-501. Such information over ten years old shall be subject to mandatory review for declassification. Requests for mandatory review shall be processed in accordance with procedures developed by the Archivist of the United States. These procedures shall provide for consultation with agencies having primary subject matter interest. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council through the process set forth in Section 3-104.</p>	<p>SEC 3.4 <u>Mandatory Review for Declassification.</u></p> <p>(a) Except as provided in Section 3.4(b), all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if:</p> <ol style="list-style-type: none"> (1) the request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and (2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort. <p>(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President, including such information in the possession and control of the Administrator of General Services pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code, is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have authority to review and declassify such information. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified until the appeal is decided.</p> <p>(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized under applicable law.</p> <p>(d) Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request.</p>	<p>Section 3.4(a) of the proposed Order contains editorial changes. Requests are now linked to the Administration's recommended changes in the FOIA. Only United States citizens etc. are authorized to request information.</p> <p>Section 3.4(b) of the proposed Order reflects the requirements of the Presidential Records Act of 1978.</p> <p>Section 3.4(c) of the proposed Order contains editorial changes to the last portion of Section 3-501 of the present Order.</p> <p>Section 3.4(d) of the proposed Order contains editorial changes to the language used in a portion of section 3-501 of the present Order.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

15

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>3-502. Requests for declassification which are submitted under the provisions of the Freedom of Information Act shall be processed in accordance with the provisions of that Act.</p> <p>3-505. No agency in possession of a classified document may, in response to a request for the document made under the Freedom of Information Act or this Order's Mandatory Review provision, refuse to confirm the existence or non-existence of the document, unless the fact of its existence or non-existence would itself be classifiable under this Order.</p> <p>3-504. Requests for declassification of classified documents originated by an agency but in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be referred by the Archivist to the agency of origin for processing in accordance with Section 3-501 and for direct response to the requestor. The Archivist shall inform requestors of such referrals.</p> <p>3-A. Downgrading.</p> <p>3-601. Classified information that is marked for automatic downgrading is downgraded accordingly without notification to holders.</p> <p>3-602. Classified information that is not marked for automatic downgrading may be assigned a lower classification designation by the originator or by other authorized officials when such downgrading is appropriate. Notice of downgrading shall be provided to holders of the information to the extent practicable.</p>	<p>(e) The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.</p> <p>(f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:</p> <p>(1) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.</p> <p>(2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.</p>	<p>Section 3.4(e) of the proposed Order is a restatement of Section 3-403 of the present Order. Section 3.4(f) of the proposed Order is restated in the positive rather than negative fashion of the present Order.</p> <p>Section 3.4(f)(1) of the proposed Order contains editorial changes.</p> <p>Section 3.4(f)(2) of the proposed Order contains editorial changes.</p> <p>Section 3-6 of the present Order has been dropped because downgrading is otherwise covered.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

16

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>SECTION 4. SAFEGUARDING.</p> <p>4-1. <i>General Restrictions on Access.</i></p> <p>4-101. No person may be given access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties.</p> <p>4-102. All classified information shall be marked conspicuously to put users on notice of its current classification status and, if appropriate, to show any special distribution or reproduction restrictions authorized by this Order.</p> <p>4-103. Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, and transmitted only under conditions that will provide adequate protection and prevent access by unauthorized persons.</p> <p>4-104. Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of Chapters 31 and 33 of Title 44 of the United States Code, which governs disposition of Federal records.</p> <p>4-105. Classified information disseminated outside the Executive branch shall be given protection equivalent to that afforded within the Executive branch.</p>	<p>PART 4</p> <p>SAFEGUARDING</p> <p>SEC 4.1 <u>General Restrictions on Access.</u></p> <p>(a) A person is eligible for access to classified information provided that a formal determination of trustworthiness has been made by agency heads or designated senior officials and provided that such access is essential to the accomplishment of authorized and lawful Government purposes.</p> <p>(b) Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.</p> <p>(c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.</p> <p>(d) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. This Section shall not be construed as reducing the authority of the Attorney General, with the advice of appropriate agency heads and subject to review by the President, to determine if the use of classified information is required to support legal proceedings. For purposes of this Section, the Department of Defense shall be</p>	<p>Section 4.1(a) of the proposed Order contains editorial changes.</p> <p>Section 4-102 of the present Order has been deleted. This subject is included under Section 1.5 of the proposed Order.</p> <p>Section 4-104 of the present Order has been deleted. This subject will be addressed in more detail in the implementing directive.</p> <p>Section 4.1(c) of the proposed Order contains editorial changes.</p> <p>Section 4.1(d) of the proposed Order is presently addressed in ISOO Directive No. 1, E.O. 12065. It more properly belongs in this section of the proposed Order.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

17

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>4-2. <i>Special Access Programs.</i></p> <p>4-201. Agency heads listed in Section 1-201 may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or prior Orders. Such programs may be created or continued only by written direction and only by those agency heads and, for matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Classified information in such programs shall be declassified according to the provisions of Section 3.</p> <p>4-202. Special access programs may be created or continued only on a specific showing that:</p> <ul style="list-style-type: none"> (a) normal management and safeguarding procedures are not sufficient to limit need-to-know or access; (b) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and (c) the special access controls balance the need to protect the information against the full spectrum of needs to use the information. <p>4-203. All special access programs shall be reviewed regularly and, except those required by treaty or international agreement, shall terminate automatically every five years unless renewed in accordance with the procedures in Section 4-2.</p> <p>4-204. Within 180 days after the effective date of this Order, agency heads shall review all existing special access programs under their jurisdiction and continue them only in accordance with the procedures in Section 4-2. Each of those agency heads shall also establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office shall have non-delegable access to all such accountings.</p>	<p>SEC 4.2 <u>Special Access Programs.</u></p> <p>(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. For special access programs pertaining to cryptology, this function will be exercised by the Secretary of Defense.</p> <p>(b) Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4) shall have non-delegable access to all such accountings.</p>	<p>Section 4.2(a) of the proposed Order contains editorial changes.</p> <p>Section 4-202 of the present Order has been deleted. This section will be addressed in the implementing directive.</p> <p>Section 4-203 of the present Order has been deleted. Continuance of this requirement is an unnecessary and costly administrative burden.</p> <p>Section 4.2(b) of the proposed Order contains editorial changes.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

18

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>4-3. <u>Access by Historical Researchers and Former Presidential Appointees.</u></p> <p>4-301. The requirement in Section 1-101 that access to classified information may be granted only as is necessary for the performance of official duties may be waived as provided in Section 4-302 for persons who:</p> <p>(a) are engaged in historical research projects, or</p> <p>(b) previously have occupied policy-making positions to which they were appointed by the President.</p> <p>4-302. Waivers under Section 4-301 may be granted only if the agency with jurisdiction over the information:</p> <p>(a) makes a written determination that access is consistent with the interests of national security;</p> <p>(b) takes appropriate steps to ensure that access is limited to specific categories of information over which that agency has classification jurisdiction;</p> <p>(c) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed or received while serving as a Presidential appointee.</p> <p>4-4. <u>Reproduction Controls.</u></p> <p>4-401. Top Secret documents may not be reproduced without the consent of the originating agency unless otherwise marked by the originating office.</p> <p>4-402. Reproduction of Secret and Confidential documents may be restricted by the originating agency.</p> <p>4-403. Reproduced copies of classified documents are subject to the same accountability and controls as the original documents.</p> <p>4-404. Records shall be maintained by all agencies that reproduce paper copies of classified documents to show the number and distribution of reproduced copies of all Top Secret documents, of all documents covered by special access programs distributed outside the originating agency, and of all Secret and all Confidential documents which are marked with special dissemination and reproduction limitations in accordance with Section 1-306.</p> <p>4-405. Sections 4-401 and 4-402 shall not restrict the reproduction of documents for the purpose of facilitating review for declassification. However, such reproduced documents that remain classified after review must be destroyed after they are used.</p>	<p>SEC 4.3 <u>Access by Historical Researchers and Former Presidential Appointees.</u></p> <p>(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who:</p> <p>(1) are engaged in historical research projects, or</p> <p>(2) previously have occupied policy-making positions to which they were appointed by the President.</p> <p>(b) Waivers under Section 4.3(a) may be granted only if the originating agency:</p> <p>(1) determines in writing that access is consistent with the interest of national security;</p> <p>(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and</p> <p>(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.</p>	<p>Section 4.3(b) of the proposed Order contains editorial changes.</p> <p>Section 4-4 of the present Order has been deleted. This section will be addressed in the implementing directive.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

19

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>SECTION 5. IMPLEMENTATION AND REVIEW.</p> <p>5-1. Oversight.</p> <p>5-101. The National Security Council may review all matters with respect to the implementation of this Order and shall provide overall policy direction for the information security program.</p> <p>5-102. The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. This responsibility shall be delegated to an Information Security Oversight Office.</p> <p>5-2. Information Security Oversight Office.</p> <p>5-201. The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Administrator also shall have authority to appoint a staff for the Office.</p> <p>5-202. The Director shall:</p> <p>(a) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order which shall be binding on the agencies;</p> <p>(b) oversee agency actions to ensure compliance with this Order and implementing directives;</p> <p>(c) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first;</p> <p>(d) have the authority to conduct on-site reviews of the information security program of each agency that handles classified information and to require of each agency such reports, information, and other cooperation as necessary to fulfill his responsibilities. If such reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect until the appeal is decided or until one year from the date of the denial, whichever occurs first.</p>	<p>PART 5</p> <p>IMPLEMENTATION AND REVIEW</p> <p>SEC 5.1 <u>Policy Direction.</u></p> <p>(a) The National Security Council shall provide overall policy direction for the information security program.</p> <p>(b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.</p> <p>SEC 5.2 <u>Information Security Oversight Office.</u></p> <p>(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.</p> <p>(b) The Director shall:</p> <p>(1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order which shall be binding on the agencies;</p> <p>(2) oversee agency actions to ensure compliance with this Order and implementing directives;</p> <p>(3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect until the appeal is decided;</p> <p>(4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a)(1) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect until the appeal is decided.</p>	<p>Section 5.1(a) of the proposed Order contains editorial changes.</p> <p>Section 5.1(b) of the proposed Order contains editorial changes.</p> <p>Section 5.2(a) of the proposed Order contains editorial changes.</p> <p>Section 5.2(b) of the proposed Order contains editorial changes.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

20

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>(g) exercise case-by-case classification authority in accordance with Section 1-205 and review requests for original classification authority from agencies or officials not granted original classification authority under Section 1-2 of this Order; and</p> <p>(h) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program, including appeals from decisions on declassification requests pursuant to Section 3-303;</p> <p>(i) report annually to the President through the Administrator of General Services and the National Security Council on the implementation of this Order;</p> <p>(j) exercise the authority to declassify information provided by Sections 3-104 and 3-303;</p> <p>3-3. <i>Interagency Information Security Committee.</i></p> <p>3-301. There is established an Interagency Information Security Committee which shall be chaired by the Director and shall be composed of representatives of the Secretaries of State, Defense, Treasury, and Energy, the Attorney General, the Director of Central Intelligence, the National Security Council, the Domestic Policy Staff, and the Archivist of the United States.</p> <p>3-302. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies.</p> <p>3-303. The Committee shall meet at the call of the Chairman or at the request of a member agency and shall advise the Chairman on implementation of this order.</p>	<p>(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;</p> <p>(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program;</p> <p>(7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program;</p> <p>(8) exercise case-by-case classification authority in accordance with Section 1.2(a);</p> <p>(9) report at least annually to the President through the National Security Council on the implementation of this Order; and</p> <p>(10) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.</p>	<p>Section 5.2(b)(7) of the proposed Order has been added to ISOO responsibilities in the interest of promoting standardization, security, and economy in security forms.</p> <p>Section 5.2(b)(10) of the proposed Order provides a more flexible means of discussing information security matters with affected agencies through ad hoc committees. The inclusion of this subsection makes Section 5-3 of the present Order unnecessary.</p> <p>Section 5-3 of the present Order has been deleted. This subject is incorporated in Section 5.2(b)(10) of the proposed Order.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

21

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>5-4. <u>General Responsibilities.</u></p> <p>5-401. A copy of any information security regulation and a copy of any guideline for systematic declassification review which has been adopted pursuant to this Order or implementing directives, shall be submitted to the Information Security Oversight Office. To the extent practicable, such regulations and guidelines should be unclassified.</p> <p>5-404. Agencies which originate or handle classified information shall:</p> <p>(a) designate a senior agency official to conduct an active oversight program to ensure effective implementation of this Order;</p> <p>5-402. Unclassified regulations that establish agency information security policy and unclassified guidelines for systematic declassification review shall be published in the <u>FEDERAL REGISTER</u>.</p> <p>(f) establish procedures to prevent unnecessary access to classified information, including procedures which require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and which ensure that the number of people granted access to classified information is reduced to and maintained at the minimum number that is consistent with operational requirements and needs; and</p> <p>5-403. Agencies with original classification authority shall promulgate guides for security classification that will facilitate the identification and uniform classification of information requiring protection under the provisions of this Order.</p> <p>5-401. (b) designate a senior agency official to chair an agency committee with authority to act on all suggestions and complaints with respect to the agency's administration of the information security program.</p>	<p>SEC 5.3 <u>General Responsibilities.</u></p> <p>(a) Agencies that originate or handle classified information shall:</p> <p>(1) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;</p> <p>(2) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published or incorporated by reference in the Federal Register to the extent that these regulations affect members of the public;</p> <p>(3) establish procedures to prevent unnecessary access to classified information, including procedures that (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs; and</p> <p>(4) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.</p>	<p>Section 5-401 of the present Order has been deleted. This section is incorporated in 5.2(b)(3) of the proposed Order.</p> <p>Section 5.3(a) of the proposed Order contains editorial changes.</p> <p>Section 5-403 of the present Order has been deleted. This subject is addressed in Section 2.2 of the proposed Order.</p> <p>Section 5-404(b) of the present Order has been deleted. This subject is incorporated in 5.3(a)(1) of the proposed Order.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

22

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>(c) establish a process to decide appeals from denials of declassification requests submitted pursuant to Section 3-3;</p> <p>(d) establish a program to familiarize agency and other personnel who have access to classified information with the provisions of this Order and implementing directives. This program shall impress upon agency personnel their responsibility to exercise vigilance in complying with this Order. The program shall encourage agency personnel to challenge, through Mandatory Review and other appropriate procedures, those classification decisions they believe to be improper;</p> <p>(e) promulgate guidelines for systematic review in accordance with Section 3-402;</p> <p>(g) ensure that practices for safeguarding information are systematic reviewed and that those which are duplicative or unnecessary are eliminate</p> <p>5-405. Agencies shall submit to the Information Security Oversight Office such information or reports as the Director of the Office may find necessary to carry out the Office's responsibilities.</p> <p>5-5. <u>Administrative sanctions.</u></p> <p>5-501. If the Information Security Oversight Office finds that a violation of this Order or any implementing directives may have occurred, it shall make a report to the head of the agency concerned so that corrective steps may be taken.</p> <p>5-502. Officers and employees of the United States Government shall be subject to appropriate administrative sanctions if they:</p> <p>(a) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directives; or</p> <p>(b) knowingly, willfully and without authorization disclose information properly classified under this Order or prior Orders or compromise properly classified information through negligence; or</p> <p>(c) knowingly and willfully violate any other provision of this Order or implementing directive.</p>	<p>SEC 5.4 <u>Sanctions.</u></p> <p>(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official designated under Section 5.3(a)(1) so that corrective steps, if appropriate, may be taken.</p> <p>(b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they:</p> <p>(1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders;</p> <p>(2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or</p> <p>(3) knowingly and willfully violate any other provision of this Order or implementing directive.</p>	<p>Section 5-404(c) of the present Order has been deleted. This subject is incorporated in 3.4(d) of the proposed Order.</p> <p>Section 5-404(d) of the present Order has been deleted. This subject is incorporated in 5.3(a)(1) of the proposed Order.</p> <p>Section 5-404(e) of the present Order has been deleted. This subject is incorporated in 3.3(a) of the proposed Order.</p> <p>Section 5-404(g) of the present Order has been deleted. This subject is incorporated in Part 4 of the proposed Order.</p> <p>Section 5-405 of the present Order has been deleted. This subject is incorporated in Section 5.2 of the proposed Order.</p> <p>Section 5.4(a) of the proposed Order contains editorial changes.</p> <p>Section 5.4(b) of the proposed Order contains editorial changes.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

23

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>5-505. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulations.</p> <p>2-501. Agency heads shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5-502 occurs. The Director of the Information Security Oversight Office shall be informed when such violations occur.</p> <p>2-505. Agency heads shall report to the Attorney General evidence reflected in classified information of possible violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General.</p>	<p>(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information or other sanction in accordance with applicable law and agency regulation.</p> <p>(d) Each agency head or the senior official designated under Section 5.36(a)(1) shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b)(1) or (2) occurs.</p>	<p>Section 5.4(d) of the proposed Order contains editorial changes.</p> <p>Section 5-505 of the present Order has been deleted. This subject is addressed in Attorney General guidelines making it redundant and inappropriate in the proposed Order.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

24

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>SECTION 8. GENERAL PROVISIONS.</p> <p>4-1. <i>Definitions.</i></p> <p>6-101. "Agency" has the meaning defined in 5 U.S.C. 552(e).</p> <p>6-102. "Classified information" means information or material, hereinafter collectively termed information, that is owned by, produced for or by, or under the control of, the United States Government, and that has been determined pursuant to this Order or prior Orders to require protection against unauthorized disclosure, and that is so designated.</p> <p>6-103. "Foreign government information" means information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement requiring confidentiality with a foreign government or international organization of governments.</p> <p>6-104. "National security" means the national defense and foreign relations of the United States.</p> <p>6-105. "Declassification event" means an event which would eliminate the need for continued classification.</p>	<p>PART 6</p> <p>GENERAL PROVISIONS</p> <p>SEC. 6.1 <u>Definitions.</u></p> <p>(a) "Agency" has the meaning provided at 5 U.S.C. 552(e).</p> <p>(b) "Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced by, produced for, or is under the control of the United States Government.</p> <p>(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.</p> <p>(d) "Foreign government information" means:</p> <p>(1) information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or</p> <p>(2) any information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or organization of governments, requiring that the information, the arrangement, or both, be held in confidence.</p> <p>(e) "National security" means the national defense and/or foreign relations of the United States.</p> <p>(f) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.</p> <p>(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.</p>	<p>This section of the proposed Order contains some editorial changes and includes three new definitions and deletes one.</p> <p>New definitions: Proposed Order: 6.1(b) Information 6.1(f) Confidential Source 6.1(g) Original Classification</p> <p>These definitions were added to insure consistent interpretation by affected agencies.</p> <p>Deleted definitions: Present Order: 6-105 Declassification Event</p> <p>This definition is self explanatory, thus including it under definitions in Section 6 of the proposed Order is unnecessary.</p>

COMPARISON OF EXECUTIVE ORDER 12065 AND THE DRAFT ORDER

25

EXECUTIVE ORDER 12065	DRAFT ORDER	REASONS FOR CHANGE
<p>6-2 General.</p> <p>6-201. Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, "Restricted Data" and information designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued pursuant thereto.</p> <p>6-202. The Attorney General, upon request by the head of an agency, his duly designated representative, or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect to any question arising in the course of its administration.</p>	<p>SEC 6.2 <u>General.</u></p> <p>(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.</p> <p>(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect to any question arising in the course of its administration.</p> <p>(c) Executive Order No. 12065 of June 28, 1978; the accompanying presidential Order of June 28, 1978; Information Security Oversight Office Implementing Directive No. 1 of October 2, 1978; and Section 5-209 of Executive Order No. 12148 of July 20, 1979, are revoked as of the effective date of this Order.</p> <p>(d) This Order shall become effective on _____.</p>	